

1 **CLAIMS:**

2 Having thus described our invention, what we claim as
3 new and desire to secure by Letters Patent is as
4 follows:

5 1. A method comprising:

6 enabling at least one client to access restricted
7 information from an origin web-server through a
8 semi-trusted web-server including the steps of:

9 authenticating said at least one client;

10 creating a client credential having client-specific
11 environment information for each said at least one
12 client;

13 presenting the client credential to the semi-trusted
14 web-server;

15 correlating said at least one client with the client
16 credential; and

17 providing said access to said at least one client.

18 2. A method as recited in claim 1, further comprising
19 serving the restricted information to said at least one
20 client through the semi-trusted web-server.

1 3. A method as in claim 1, wherein the step of
2 creating comprises storing the client-specific
3 environment information and the client credential in a
4 cookie in said at least one client's browser.

5 4. A method as in claim 1, wherein the step of
6 presenting comprises:

7 sending the client credential to the semi-trusted
8 web-server; and

9 using HTTP redirection to refer said at least one
10 client to the semi-trusted web-server.

11 5. A method as in claim 1, wherein the step of
12 presenting comprises:

13 sending said at least one client credential to a
14 directory accessible to the semi-trusted web-server;
15 and

16 the origin web-server using HTTP redirection to send
17 said at least one client to the semi-trusted
18 web-server.

19 6. A method as in claim 1, wherein the step of creating
20 comprises:

21 collecting the client-specific environment information;
22 and

1 storing the client-specific environment information in
2 the client credential.

3 7. A method as in claim 6, wherein the client-specific
4 environment information includes:

5 a hash of the HTTP-Request header of said at least one
6 client request;

7 a hash of the IP address of the machine used by said at
8 least one client;

9 a process identity of said at least one client browser;

10 a hash of a user identity used by said at least one
11 client program; and/or

12 any combination of these.

13 8. A method as in claim 1, wherein the step of
14 creating comprises:

15 placing a first client-side program at said at least
16 one client;

17 collecting a first set of the client-specific
18 environment information using the first client-side
19 program;

20 sending the first set of the client-specific
21 environment information to the origin web-server; and

1 storing the first set of the client-specific
2 environment information in the client credential.

3 9. A method as in claim 8, wherein the step of
4 correlating includes:

5 the semi-trusted web-server placing a second
6 client-side program at said at least one client;

7 collecting a second set of the client-specific
8 environment information with the second client-side
9 program;

10 sending the second set of the client-specific
11 environment information to the semi-trusted
12 web-server; and

13 correlating the second set of the client-specific
14 environment information to the client credential.

15 10. A method as in claim 9, wherein the first and/or
16 the second client-specific environment information
17 includes: a hash of the HTTP-Request header of said at
18 least one client request; a hash of the IP address of
19 the machine used by said at least one client; a process
20 identity of said at least one client browser; a hash of
21 a user identity used by said at least one client
22 program; and/or any combination of these.

23 11. A method as in claim 1, further comprising the
24 semi-trusted web-server accessing an encrypted version
25 of the restricted information, and wherein the step of

1 creating the client credential includes adding a
2 decryption key to the client credential.

3 12. A method as in claim 11 wherein the decryption key
4 is a partial key, and the step of providing includes
5 the semi-trusted web-server supplying information to
6 said at least one client enabling conversion of the
7 partial key to a full key.

8 13. A method as in claim 1 wherein the step of
9 authenticating includes employing a user-password
10 scheme.

11 14. A method as in claim 1, wherein the step of
12 authenticating includes deploying at least one
13 certificate.

14 15. A method as in claim 6, wherein the step of
16 collecting the client-specific environment information
is performed by the origin web-server, and

17 the origin web-server storing the client-specific
18 environment information in the client credential.

19 20 21 16. A method as in claim 8, wherein the steps of
placing and the step of storing is performed by the
origin web-server.

22 23 17. A method as recited in claim 1, wherein the
semi-trusted web-server is a proxy web-server.

1 18. A method as recited in claim 1, wherein the step of
2 creating a credential for said at least one client at
3 an origin web-server;

4 19. A method as recited in claim 1, wherein the step
5 of correlating said at least one client and the client
6 credential is performed by the semi-trusted web-server.

7 20. A method as recited in claim 1, wherein the step of
8 authenticating said at least one client is performed at
9 the origin web-server.

10 21. An apparatus for enabling at least one client to
11 access restricted information from an origin web-server
12 through a semi-trusted web-server, said apparatus
13 comprising:

14 an authenticator to validate said at least one client;

15 a credential creator to create a client credential
16 having client-specific environment information for each
17 said at least one client; and

18 a correlator for matching said at least one client to
19 the client credential.

20 22. The apparatus as in claim 21, wherein the
21 credential creator stores the client-specific
22 environment information in a cookie set in said at
23 least one client's browser.

1 23. An apparatus as in claim 21, wherein the credential
2 creator presents the credential to the semi-trusted
3 web-server.

4 24. The apparatus as in claim 21, wherein the
5 credential creator stores a client-side program in said
6 at least one client's browser.

7 25. The apparatus as in claim 21, wherein the
8 correlator stores a second client-side program in the
9 client's browser.

10 26. The apparatus as in claim 21, wherein the
11 semi-trusted web-server has access only to an encrypted
12 version of the restricted information, and the
13 credential creator adds a decryption key to the client
14 credential.

15 27. The apparatus as in claim 26, wherein the
16 decryption key is a partial key and the semi-trusted
17 web-server includes an information supplier to supply
18 said at least one client with information to enable
19 conversion of the partial key to a full key.

20 28. An article of manufacture comprising a computer
21 usable medium having computer readable program code
22 means embodied therein for enabling at least one client
23 to access restricted information from an origin
24 web-server through a semi-trusted web-server, the
25 computer readable program code means in said article of
26 manufacture comprising computer readable program code

1 means for causing a computer to effect the steps of
2 claim 1.

3 29: An article of manufacture as recited in claim 28,
4 the computer readable program code means in said
5 article of manufacture further comprising computer
6 readable program code means for causing a computer to
7 effect the steps of claim 12.

8 30. A program storage device readable by machine,
9 tangibly embodying a program of instructions executable
10 by the machine to perform method steps for enabling at
11 least one client to access restricted information from
12 an origin web-server through a semi-trusted web-server,
13 said method steps comprising the steps of claim 1.

14 31. An apparatus comprising:

15 means for enabling at least one client to access
16 restricted information from an origin web-server
17 through a semi-trusted web-server including:

18 means for authenticating said at least one client;

19 means for creating a client credential having
20 client-specific environment information for each said
21 at least one client;

22 means for presenting the client credential to the
23 semi-trusted web-server;

1 means for correlating said at least one client with the
2 client credential; and

3 means for providing said access to said at least one
4 client.

5 32. An apparatus as recited in claim 31, further
6 comprising means for serving the restricted information
7 to said at least one client through the semi-trusted
8 web-server.

9 33. An apparatus as in claim 31, further comprising
10 means for storing the client-specific environment
11 information and the client credential in a cookie in
12 said at least one client's browser.

13 34. An apparatus as in claim 31, further comprising
14 means for:

15 sending the client credential to the semi-trusted
16 web-server; and

17 using HTTP redirection to refer said at least one
18 client to the semi-trusted web-server.

19 35. An apparatus as in claim 31, wherein the origin
20 web-server uses HTTP redirection to send said at least
21 one client to the semi-trusted web-server, and further
22 comprising means for sending said at least one client
23 credential to a directory accessible to the
24 semi-trusted web-server.

1 36. An apparatus as in claim 31, further comprising
2 means for:

3 collecting the client-specific environment information;
4 and

5 storing the client-specific environment information in
6 the client credential.

7 37. An apparatus as in claim 36, wherein the
8 client-specific environment information includes:

9 a hash of the HTTP-Request header of said at least one
10 client request;

11 a hash of the IP address of the machine used by said at
12 least one client;

13 a process identity of said at least one client browser;

14 a hash of a user identity used by said at least one
15 client program; and/or

16 any combination of these.

17 38. An apparatus as in claim 31, further comprising
18 means for:

19 placing a first client-side program at said at least
20 one client;

1 collecting a first set of the client-specific
2 environment information using the first client-side
3 program;

4 sending the first set of the client-specific
5 environment information to the origin web-server; and

6 storing the first set of the client-specific
7 environment information in the client credential.

8 39. An apparatus as in claim 38, further comprising
9 means for:

10 the semi-trusted web-server to place a second
11 client-side program at said at least one client;

12 collecting a second set of the client-specific
13 environment information with the second client-side
14 program;

15 sending the second set of the client-specific
16 environment information to the semi-trusted web-server;
17 and

18 correlating the second set of the client-specific
19 environment information to the client credential.

20 40. An apparatus as in claim 39, wherein the first
21 and/or the second client-specific environment
22 information includes:

1 a hash of the HTTP-Request header of said at least one
2 client request;

3 a hash of the IP address of the machine used by said at
4 least one client;

5 a process identity of said at least one client browser;

6 a hash of a user identity used by said at least one
7 client program;

8 and/or any combination of these.

9 41. An apparatus as in claim 31, further comprising
10 means for the semi-trusted web-server to access an
11 encrypted version of the restricted information, and
12 means for adding a decryption key to the client
13 credential during creation.

14 42. An apparatus as in claim 41, wherein the decryption
15 key is a partial key comprising means for the
16 semi-trusted web-server to supply information to said
17 at least one client enabling conversion of the partial
18 key to a full key.

19 43. An apparatus as in claim 31, further comprising of
20 a means for authenticating by employing a user-password
21 scheme.

22 44. An apparatus as in claim 31, further comprising of
23 a means for authenticating by deploying at least one
24 certificate.

1 45. A computer program product comprising a computer
2 usable medium having computer readable program code
3 means embodied therein for causing enablement of at
4 least one client to access restricted information from
5 an origin web-server through a semi-trusted web-server,
6 the computer readable program code means in said
7 computer program product comprising computer readable
8 program code means for causing a computer to effect the
9 apparatus of claim 31.

10 46. A computer program product comprising a computer
11 usable medium having computer readable program code
12 means embodied therein for causing enablement of at
13 least one client to access restricted information from
14 an origin web-server through a semi-trusted web-server,
15 the computer readable program code means in said
16 computer program product comprising computer readable
17 program code means for causing a computer to effect the
18 apparatus of claim 21.